UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/763,079	01/22/2004	Daniel Brokenshire	AUS920030972US1	6481

50170 7590 02/02/2007

IBM CORP. (WIP)
c/o WALDER INTELLECTUAL PROPERTY LAW, P.C.
P.O. BOX 832745
RICHARDSON, TX 75083

EXAMINER	
ANWARI, MACEEH	
ART UNIT	PAPER NUMBER
2109	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	02/02/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/763,079	BROKENSHIRE ET AL.	
	Examiner	Art Unit	
	Maceeh Anwari	2109	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-23 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-23 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date 1/22/04
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This is the initial Office action based on the 10/763,079 application filed January 22, 2004. Claims 1-23, as originally filed, are currently pending and have been considered below.

Specification

2. Applicant is reminded of the proper language and format for an abstract of the disclosure.

The abstract should be in narrative form and generally limited to a single paragraph on a separate sheet within the range of 50 to 150 words. It is important that the abstract not exceed 150 words in length since the space provided for the abstract on the computer tape used by the printer is limited. The form and legal phraseology often used in patent claims, such as "means" and "said," should be avoided. The abstract should describe the disclosure sufficiently to assist readers in deciding whether there is a need for consulting the full patent text for details.

The language should be clear and concise and should not repeat information given in the title. It should avoid using phrases which can be implied, such as, "The disclosure concerns," "The disclosure defined by this invention," "The disclosure describes," etc.

3. The abstract of the disclosure is objected to because the abstract is 247 words, which is greater than the 150 allowed (see above). Correction is required. See MPEP § 608.01(b).

Claim Objections

4. Claim 21 is objected to because of the following informalities: it uses the word “system,” instead of “method” or process when referring to claim 18. Appropriate correction is required.

Claim Rejections - 35 USC § 101

5. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 1-23 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claims 1-11, 16-17 and 22-23 do not fall within at least one of the four categories of patent eligible subject matter; rather what the applicant has disclosed within these claims is interpreted as being software per se.

Claims 1-23 each fall under a judicial exception, an abstract idea, and are not directed to a practical application of such a judicial exception because they fail to produce a tangible result.

Further regarding claims 1-6, where claim 1 is the independent claim and 2-6 are the dependent claims, the applicant has disclosed a system; wherein the components to this system, the random value generator, the message validation code generator, the predetermined key, the one-time pad generator, and the protected message envelope are all taken to be, by the examiner, intrinsically as being software configured to perform an action but failing to provide a tangible result.

Whereas for claims 7-11, where claim 7 is the independent claim and claims 8-11 are the dependent claims the applicant once again discloses a system, comprising a protected message envelope reader, a protected message

envelope, a generated random value, a masked message, a message validation code, a one-time pad generator, a predetermined key, and a message unmasker once again are all taken to be, by the examiner, as software per se configured to perform an action but failing to provide a tangible result.

Regarding claims 12-15 and 18-21, even though these claims mention a method/process they still fail to produce a tangible result.

Paying specific attention to claims 16 and 17, the applicant is trying to claim a manufacture however, as stated a secure message fails to fall within the four categories of a useful process, machine, manufacture, or composition of matter. As claimed they fail to produce a tangible result. They also fail to claim the manufacture combined with a proper computer readable medium, and is thus software per se.

As for claims 22 and 23 they disclose a computer program product, sharing the same above mentioned components, and failing to fall under one of the statutory categories. It is software per se and fails to provide a tangible result. As the applicant is attempting to claim a manufacture, the examiner notes that the claim is lacking a proper computer readable medium.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before

the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

7. Claims 1-23 are rejected under 35 U.S.C. 102(e) as being anticipated by Shrader et al (hereinafter Shrader), U.S. Patent No. 6,914,985.

Shrader teaches:

Claim 1:

A system for secure communication, comprising: a random value generator configured to generate a random value (Col. 11, lines 47-48; teaches this because the enveloped data is constructed and generated at random); a message validation code generator (Col. 2, lines 19-29 & Col. 13, line 57-67; states that the enveloped data have validation checks) coupled to the random value generator and configured to generate a message validation code based on a predetermined key (Figure 3 & 4C & 7 & Col. 1, line 27-43; states how the Public-key cryptography standard is applied within his and other inventions), a message (Col. 2, lines19-40; teaches here that using the PKCS #7 one would be able to include encrypted messages), and the random value; a one-time pad generator coupled to the random number generator and configured to generate a one-time pad based on the random value and the predetermined key; and a masked message generator coupled to the one-time pad generator and configured to generate a masked message based on the one-time pad and the message (Col. 11, lines 65-67; meets the limitation of generating

a masked message based on the one-time pad by stating that the encrypted content/data be padded to a multiple of some block size);

Claims 2- 4:

Wherein the message validation code generator (MVC), and the one-time pad generator (OTP), employs a first one-way hash function and wherein the MVC employs a first one-way hash function and the OTP employs a second one-way hash function (Col. 8, lines 31-35 & lines 62-67 & Col. 9, lines1-2 & Col. 11, lines 47-48; teaches on the use of a single or multiple hash functions and or algorithms.)

Claim 5:

The system as recited in claim 1, further comprising a protected message envelope (PME) generator coupled to the random value generator (Col. 11, lines 46-47; meets the limitations of a PME and a random generator), the message validation code generator (Col. 2, lines 19-29 & Col. 13, lines 57-67; meets the limitations of a message validation process), and the masked message generator (Col. 13, lines 34-44; reads on an encryption messaging process), and configured to generate a protected message envelope based on the random value, the message validation code, and the masked message (the combination of the above sections and Figure 3 anticipate all the features within this claim).

Claim 6:

The system as recited in claim 5, further comprising a transmitter coupled to the protected message envelope generator and configured to

transmit the protected message envelope to a target (Col. 13, lines 57-67 & Col. 14, lines 1-7; reads on the limitations of the transmitter and transmission).

Claim 7:

A system for secure communication, comprising: a protected message envelope reader configured to receive a protected message envelope (Col. 12, lines 4-7 & Col. 15, lines 38-63; meets the limitations of protected message enveloped reader) and generate a random value, a masked message (Col. 11, lines 47-48 & 62-67 & Col. 12, lines 1-3; reads on the random value and the masked message components), and a first message validation code based on the received protected message envelope (Col. 2, lines 19-29 & Col. 13, lines 57-67; meets the limitation of the validation); a one-time pad generator coupled to the protected message envelope reader and configured to generate a one-time pad based on the random value and a predetermined key (Col. 11, lines 46-67; reads on the limitation of the pad and the key); and a message unmasker coupled to the one-time pad generator and protected message envelope reader, and configured to generate an unmasked message based on the one-time pad and the masked message (Col. 12, lines 4-7& 34-46 & Col. 15, lines 38-63; reads on the unmasking of the masked message).

Claim 8:

The system as recited in claim 7, wherein the one-time pad generator employs a first one-way hash function (Col. 8, lines 31-35 &

lines 62-67 & Col. 9, lines1-2 & Col. 11, lines 47-48; teaches on the use of a single or multiple hash functions and or algorithms).

Claim 9:

The system as recited in claim 7, further comprising a validation module (Col. 2, lines 19-29 & Col. 13, lines 57-67; meets the limitation of the validation) coupled to the protected message envelope reader (Col. 12, lines 4-7 & Col. 15, lines 38-63; meets the limitations of protected message enveloped reader) and the message unmasker (Col. 12, lines 4-7& 34-46 & Col. 15, lines 38-63; reads on the unmasking/decrypting of the masked/encrypted message), the validation module comprising: a message validation code generator configured to generate a second message validation code based on the predetermined key, the unmasked message(Col. 2, lines 19-29 & Col. 13, lines 57-67; meets the limitation of the validation/authentication of the message and the key), and the random value(Col. 11, lines 47-48; teaches this because the enveloped data is constructed and generated at random); and a message validation code comparator coupled to the protected message envelope reader and the message validation code generator and configured to generate a validation based on the first message validation code and the second message validation code(Col. 2, lines 19-29 & Col. 13, lines 57-67; meets the limitation of the validation/authentication).

Claims 10-11:

Wherein the validation module employs a first one-way hash function and wherein the validation module employs a first one-way hash function and the one-time pad generator employs a second one-way hash function (Col. 8, lines 31-35 & lines 62-67 & Col. 9, lines1-2 & Col. 11, lines 47-48; teaches on the use of a single or multiple hash functions and or algorithms).

Claim 12:

A method for secure communication, comprising: generating a random value (Col. 11, lines 47-48; teaches this because the enveloped data is constructed and generated at random); generating a message validation code based on a message, the random value, a predetermined key (Col. 2, lines 19-29 & Col. 13, lines 57-67; meets the limitation of the validation/authentication and the key), and a first one-way hash function; generating a one-time pad based on the random value (Col. 11, lines 65-67; meets the limitation of generating a masked message based on the one-time pad by stating that the encrypted content/data could be padded), the predetermined key, and a second one-way hash function; and generating a masked message based on the message and the one-time pad (Col. 8, lines 31-35 & lines 62-67 & Col. 9, lines1-2 & Col. 11, lines 47-48; teaches on the use of a single or multiple hash functions and or algorithms).

Claim 13:

The method as recited in claim 12, further comprising generating a protected message envelope based on the random value, the masked message, and the message validation code (Col. 11, lines 46-67; reads on the limitations of the protected message envelope, the random value along with the masked/encrypted message; Col. 2, lines 19-29 & Col. 13, lines 57-67 meet the limitations of the validation).

Claim 14:

The method as recited in claim 13, further comprising transmitting the protected message envelope to a target destination (Col. 13, lines 57-67 & Col. 14, lines 1-7; reads on the limitations of the transmitter and transmission).

Claim 15:

Wherein the first one-way hash function and the second one-way hash function are the same one-way hash function (Col. 8, lines 31-35 & lines 62-67 & Col. 9, lines1-2 & Col. 11, lines 47-48; teaches on the use of a single or multiple hash functions and or algorithms).

Claims 16-17:

A secure message generated by the method of claim 12 and a secure message generated by the method of claim 13 (Col. 2, lines 19-40 & Col. 3, lines 18-23 & 47-67 & Col. 11, lines 46-67 & Col. 12 lines 1-3; read on the limitations of the secure message).

Claim 18:

A method for secure communication, comprising: receiving a random value, a masked message, and a first message validation code (Col. 11, lines 46-67; reads on the limitations of the protected message envelope, the random value along with the masked/encrypted message; Col. 2, lines 19-29 & Col. 13, lines 57-67 meet the limitations of the validation); generating a one-time pad based on the random value, a predetermined key, and a first one-way hash function; and generating an unmasked message based on the one-time pad and the masked message (Col. 11, lines 65-67; meets the limitation of generating a masked message based on the one-time pad by stating that the encrypted content/data could be padded; Figure 3 & 4C & 7 & Col. 1, line 27-43 & Col. 12 lines 4-7; reads on the predetermined key limitation and the unmasking/decrypting of the masked/encrypted message).

Claim 19:

The method as recited in claim 18, further comprising: generating a second message validation code based on the unmasked message, the random value (Col. 11, lines 46-48; reads on the limitations of the random values), the predetermined key and a second one-way hash function; and comparing the first message validation code to the second message validation code to determine a validity of the unmasked message (Figures 3 & 4A-B & Col. 2 lines 19-40 & Col. 13 lines 57-67; reads on the limitations of the message validation including the decryption, the key and the hash function).

Claim 20:

The method as recited in claim 19, wherein the first one-way hash function and the second one-way hash function are the same one-way hash function (Col. 8, lines 31-35 & lines 62-67 & Col. 9, lines1-2 & Col. 11, lines 47-48; teaches on the use of a single or multiple hash functions and or algorithms).

Claim 21:

The *system* (the word method should be used here instead of system, and it is being read as a mistake by the applicant) of claim 18, further comprising: receiving a protected message envelope; and generating a random value, a masked message, and a first message validation code based on the received protected message envelope (Figure 5A-B & Col. 2 lines 19-32; reads on the limitations of receiving the protected message envelope; and by stating that the system allows for recursion, envelope nesting, and the authentication of the content of the message, reads on the limitations of the message validation).

Claim 22:

A computer program product for secure communications, the computer program product having a medium with a computer program embedded thereon (Col. 20 lines 12-23; reads on the medium), the computer program comprising: computer code for generating a random value (Col. 11, lines 46-48; reads on the limitations of the random value); computer code for generating a message validation code based on a

message to be sent, the random value, a predetermined key, and a first one-way hash function (Col. 2, lines 19-32 & Col. 11, lines 46-61; reads on the limitations of the random value, the key, and the hash function); computer code for generating a one-time pad based on the random value, the predetermined key, and a second one-way hash function (Col. 11, lines 46-67; reads on the limitations of the padded data, the random value, the key and the hash function); computer code for generating a masked message based on the message to be sent and the one-time pad; and computer code for generating a protected message envelope based on the random value, the masked message, and the message validation code (Col. 11, lines 46-67 & Col. 13, lines 57-67; has the limitations of the masked message, the padded data, the protected message envelope, the random value and the message validation).

Claim 23:

A computer program product for secure communications, the computer program product having a medium with a computer program embedded thereon (Col. 20 lines 12-23; reads on the medium), the computer program comprising: computer code for-receiving a protected message envelope; computer code for generating a random value (Col. 11, lines 46-48; reads on the limitations of the random value), a masked message, and a first message validation code based on the protected message envelope (Figure 5A-B & Col. 2 lines 19-32; reads on the limitations of receiving the protected message envelope; and by stating

that the system allows for recursion, envelope nesting, and the authentication of the content of the message, reads on the limitations of the message validation); computer code for generating a one-time pad based on the random value, a predetermined key, and a first one-way hash function (Col. 11, lines 46-67 reads on the padded data, the random value, the key and the hash function); computer code for generating an unmasked message based on the one-time pad and the masked message (Col. 11, lines 65-67 & Col. 12, lines 4-7; reads on the limitation of the padded data and the decrypting/unmasking of the message); computer code for generating a second message validation code based on the unmasked message, the random value, the predetermined key, and a second one-way hash function (Col. 2, lines 19-32 & Col. 11 lines 47-48; read on the validation irrespective of number of iterations, also reads on the random factor, the key, and the hash functions); and computer code for comparing the first message validation code to the second message validation code to determine a validity of the unmasked message (Col. 2, lines 19-32; once again read on the validation irrelevant of the number of times the data is authenticated).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Maceeh Anwari whose telephone number is 571-272-7591. The examiner can normally be reached on Monday-Friday 7:30-5:00 PM ES.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Joe Del Sole can be reached on 571-272-1130. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

***

Joseph S Del Sole
JOSEPH S. DEL SOLE
PRIMARY EXAMINER
1/22/07